IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE METHODS TO CURB CYBER ASSAULTS: A REVIEW

Kushagra Pal[1], Roopam Tiwari[2], Shivam Maheshwary[3]

[1,2,3] Department of Information Technology SVKM'S NMIMS MPSTME, Mumbai, Maharashtra, India,

---***---

Abstract - *With the advancement in technology, attackers are making use of cyberspace to perform various cyber attacks. Cyber frameworks are highly sensitive to intrusion as well as many other threats. As every workplaces now a days are connected to some network in one way or another leads to heavy traffic or network congestion, more security attack attempts and security breaches. We need to have security from these attacks. The treatment of various attacks is also accessible, but the approach to find which system is being attacked is difficult. This paper provides an introduction of the Cyber Security techniques and how Artificial Intelligence (AI) could help in solving the cyber security problems. It also shows the work done in the area of Artificial Intelligence for fighting against cyber assaults.*

***Key Words*: Artificial Intelligence (AI), Expert System, Artificial Neural Network (ANN), Intelligent System, Intrusion Detection System (IDS)**

1. INTRODUCTION

Cyber crimes are not limited to a particular area but is extended over every part of computer network across the globe. Advancement of technology are making attackers more advance in cyber crimes as they are also using the modern techniques to break into the network. The attackers identify the susceptibility existing in the Operating System, system application and operate that to damage the system [1]. Only human involvement cannot curb these threats.

Traditional security methods and algorithms cannot alone put curb on the cyber-crimes so there is the need of artificial intelligence techniques to prevent cyber-crimes. Artificial intelligence is widely used in industries to collect data and information. With the use of AI techniques that data could be processed into meaningful information which could be used to prevent cyber assaults [2].

AI provides various techniques such as Expert System, Intelligent Agents, Neural Networks, Pattern Recognition, Machine Learning, Artificial Immune Systems, etc.

2. ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY

2.1 Application of Expert System

Expert system has a knowledge base, in which all the factual and heuristic knowledge is stored. It also has an inference engine for interpreting answers relevant to the information and, likely extra information about a scenario. Knowledge base and inference engine are as one known as expert system [3].

In (2014) an Expert System was invented which along with the risk score calculation module helped to analyze, correspond and determine the threat level related with current transaction on an Electronic-commerce website [4].

With the help of drool's tool an expert system known as OPENSKe was developed. In this input data was given to system to identify and vulnerability [5].

Kerim Goztepe (2012) developed a Cyber security expert system based on fuzzy rule. Main segment in this was collection of data, stating variables i.e. insertion of data, retrieval of data and then execution [6].

D. Welch proposed attacks on wireless network classification. This was developed on the safety principles that infect and their solutions. For instance threat defying integrity, availability and confidentiality [7].

2.2 Application of Artificial Neural Network

Neural Network also known as deep learning. Frank Rosenblatt in 1957 lays the foundation of neural network with the invention of artificial neuron called perceptron [15]. These perceptron can combine with other perceptron to make neural networks. In neural network perceptron can be millions in number [8].

It is cited by Shaiqua Jabeen et al. [9] that artificial neural network simulates the processing of the brain by learning things on its own, by interpreting logics, devising logics and by proposing solutions. Artificial neural network has multilayer architecture in which the output produced by one layer of perceptron is given to another layer of perceptron.

Host based intrusion detection is proposed by Devikrishna K S et. al [10] they have proposed that during training phase various patterns are fed into the network and their associated output are recognized by the system. Neural network works by recognizing patterns that are already fed into its memory. It interprets logic by recognizing the patterns and by comparing it with the already learnt logic and tries to find the similarities in the input and already fed patterns.

Detecting cyber assaults using neural network is more advantageous as it is pretty fast in detecting the anomaly or intrusion .Because protection of computer network means timely detection of intrusion attempts so that harm to system could be minimized [10][2].

Devikrishna K S et.al (2013) introduced A Multi-Layer Perception for intrusion detection using Knowledge discovery in Database (KDD) for categorization of attacks [10].

It is cited by Nabil EL KADHI at el. [11] that the most widely used application of neural network is Intrusion Detection and Prevention System (IDPS) in which Neural network could be uses to detect cyber-crimes. In which ANN will learn all the possible attack agents and techniques in its training phase and adjusts its weights accordingly according to incoming input. Once training phase is completed, it is test by linking ANN to an in use network and corresponding output is generated which is an estimated estimation between 0 and 1.

Linda (2009) proposed a IDS based on Neural Network which uses a certain integration of two artificial neural network algorithms. Experimental results demonstrating that IDS-NNM algorithm having capability of catching all intrusion trials presented on the integrated network without generating any incorrect or untrue alerts [12].

Iftikhar (2009) designed a system based on ANN to detect probing attacks. It adopted a supervised neural network phenomenon to inspect the viability of an approach to investigate attacks that could be the basis of further attacks in network system. The system which is developed is used to find out different attacks during investigation and while comparing its performance with different neural networks‟ results indicate that approach based on Multiple Layered Perceptron (MLP) architecture is more precise and accurate and it shows most favourable results in contrast to other methods [13].

Barika (2009) proposed a comprehensive architecture of intrusion detection system based on ANN architecture for decision making within IDS with more efficiency [14].

2.3 Application of Intelligent System

Intelligent Agent (IA) are those who recognize movement with sensors and act on an environment using actuators and direct its activity for completing objectives [15].

The intelligent agent properties like mobility, flexibility in environments they are executed in, and their cooperative nature, makes them fit for combating cyber crimes [16].

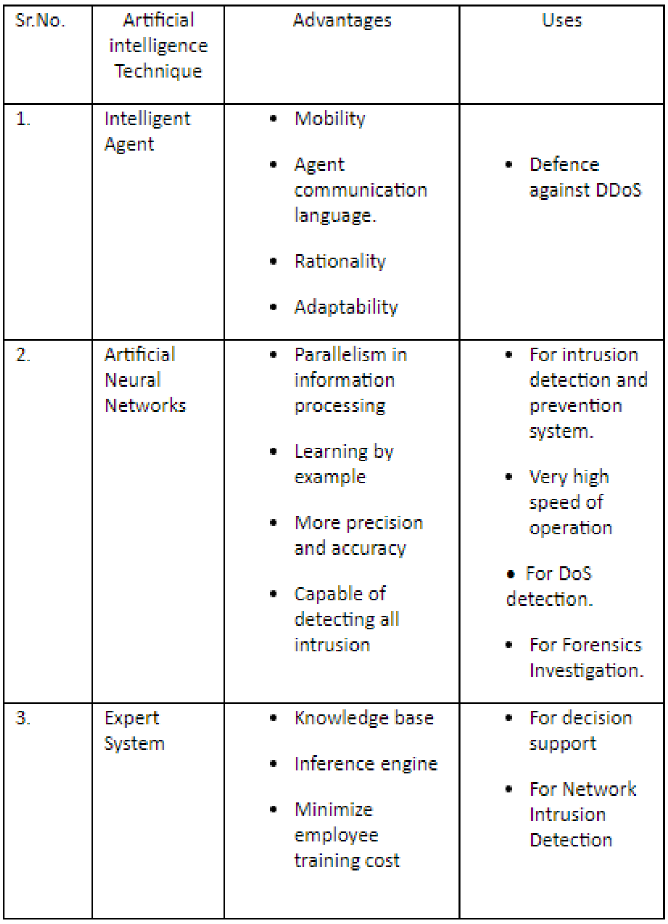
Rowe (2003) invented a tool to orderly counter plan the methods to prevent specific cyber attack plans by using multi-agent planning [17].

Helano (2006) brought in a system implemented in Prolog which is a combination based on a (MAS) multi-agent systems approach with a operable case used to defend cyber attacks and with the capability to verify the characteristics of cyber attacks [18].

Gou (2006) proposed Multi Agent System for Computer Worm Detection (MWDCM) and curbing in MANs, which spontaneously has the generation of worms which disuse a mass of network transmission capacity and crashes the router. Researches illustrated that the system efficiently curb worm transmission [19].

Edwards (2007) proposed the potency of intelligent agent techniques for enhancing the activity of power grids, thwarting known crimes and rationalize their results. They proposed a Multi Layered Security Model (MLSM) prototype that gives defense from invalid input and capability to find and retrieve from unknown crime techniques [20].

Kotenko et al. (2010) researched multi-agent based progresses to the examination and protection against botnets which are increasingly growing across the network and being use to curb numerous cyber attacks like executing vulnerability scans, distributed Denial of Service attacks, and sending large number of spam mails. They outlined the infrastructure and execution attributes of such systems [21].



Sr.No.	Artificial intelligence Technique	Advantages	Uses
1.	Intelligent Agent	• Mobility • Agent communication language. • Rationality • Adaptability	• Defence against DDoS
2.	Artificial Neural Networks	• Parallelism in information processing • Learning by example • More precision and accuracy • Capable of detecting all intrusion	• For intrusion detection and prevention system. • Very high speed of operation • For DoS detection. • For Forensics Investigation.
3.	Expert System	• Knowledge base • Inference engine • Minimize employee training cost	• For decision support • For Network Intrusion Detection

3. CONCLUSIONS AND FUTURE WORK

As we live in a modernized world, most of our everyday communications and commercial activities take place via the Internet. However, it also causes issues which are hard to handle such as the emergence of cyber-attacks on computer networks. At hand academic resources show that AI methods already have various implementation to tackle cybercrimes. This paper concisely introduced possibilities of AI techniques so far in cyber field for combating cyber crimes and their current limitations [16].

With the enhancement of technology day by day hackers are also growing smart. May be in future hackers also tries to use the various ways of artificial intelligence to break into network or system.

In future we look forward to realize a part of the cyber defense structure (CDS) with the help of programmable logic arrays. Such means of solving an intrusion detection problem, unlike the software protection, will enable to remove the impact of the software intrusions on the Cyber defense structure [22].

REFERENCES

[1] Cheshta Rani , Shivani Goel. An Expert System for Cyber Security Attack Awareness, International Conference on Computing, Communication and Automation (ICCCA2015) ISBN:978-1-4799-8890-7/15/$31.00 ©2015 IEEE 242 CSAAES.

[2] A. S. Poonia, A. Bhardwaj, G. S. Dangayach, (2011) “Cyber Crime: Practices and Policies for Its Prevention”, The First International Conference on Interdisciplinary Research and Development, Special No. of the International Journal of the Computer, the Internet and Management, Vol. 19, No. SP1.

[3] Dr. Sunil Bhutada,Preeti Bhutada.Applications of Artificial Intelligence in Cyber security International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 4, April 2018 All Rights Reserved © 2018 IJERCSE 214 .

[4] NIKITA RANA, SHIVANI DHAR,PRIYANKA JAGDALE, NIKHIL JAVALKAR. Implementation of An Expert System for the Enhancement of E-Commerce Security International Journal of Advances in Science Engineering and Technology, ISSN: 2321-9009 Volume- 2, Issue-3, July-2014

[5] M.M. Gamal, B. Hasan, and A.F. Hegazy, “A Security Analysis Framework Powered by an Expert System,” International Journal of Computer Science and Security (IJCSS), Vol. 4, no. 6, pp. 505-527, Feb. 2011.

[6] K. Goztepe, “Designing a Fuzzy Rule Based Expert System for Cyber Security,” International Journal Of Information Security Science, vol.1, no.1, 2012 .

[7] D. Welch, “Wireless Security Threat Taxonomy,” Information Assurance Workshop. IEEE Systems, Man and Cybernetics Society, pp 76-83, June 2003.

[8] Vidushi Sharma ,Sachin Rai, Anurag Dev” A Comprehensive Study of Artificial Neural Networks” International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 10, October 2012.

[9] Shaiqua Jabeen , Shobhana D. Patil, Shubhangi V. Bhosale , Bharati M. Chaudhari, Prafulla S. Patil” A Study on Basics of Neural Network” International Journal of Innovative Research in Computer and Communication Engineering Vol. 5, Issue 4, April 2017.

[10] Devikrishna K S, Ramakrishna B B “An Artificial Neural Network based Intrusion Detection System and Classification of Attacks”International Journal of Engineering Research and Applications (IJERA) Vol. 3, Issue 4, Jul-Aug 2013, pp. 1959-1964.

[11] Nabil EL KADHI, Karim HADJAR, Nahla EL ZANT ” A Mobile Agents and Artificial Neural Networks for Intrusion Detection” JOURNAL OF SOFTWARE, VOL. 7, NO. 1, JANUARY 2012.

[12] Linda Ondrej, T. Vollmer, M. Manic, (2009) “Neural Network Based Intrusion Detection System for Critical Infrastructures”, Proceedings of International Joint Conference on Neural Networks, pp. 1827 1834.

[13] A. Iftikhar, B.A. Azween, A. S. Alghamdi, (2009) “Application of artificial neural network in detection of dos attacks,” Proceedings of the 2nd ACM international conference on Security of information and networks, pp. 229–234.

[14] F. Barika, K. Hadjar, N. El-Kadhi, (2009) “Artificial neural network for mobile IDS solution”,Security and Management, pp. 271–277.

[15] Arockia Panimalar.S, Giri Pai.U, Salman Khan.K “ARTIFICIAL INTELLIGENCE TECHNIQUES FOR CYBER SECURITY” International Research Journal of Engineering and Technology (IRJET)Volume: 05 Issue: 03 | Mar-2018 .

[16] Jyothsna S Mohan, Nilina ,”Prospects of Artificial Intelligence in Tackling Cyber Crimes” International Journal of Science and Research (IJSR) Volume 4 Issue 6, June 2015.

[17] IEEE Workshop on Information Assurance, pp. 203 210.

[18] José Helan and Matos Nogueira, ”Mobile Intelligent Agents to Fight Cyber Intrusions”, International Journal of Forensic Computer Science , IJoFCS, pp 28-32,2006.

[19] X. Gou, W. Jin, D. Zhao, (2006) "Multi-agent system for worm detection and containment in metropolitan area networks", Journal of Electronics, Vol. 23, No. 2, pp. 259-265.

[20] D. Edwards, S. Simmons, N. Wilde, (2007) “Prevention, Detection and Recovery from Cyber-Attacks Using a Multilevel Agent Architecture”, IEEE International Conference on System of Systems Engineering (SoSE '07), pp. 1 – 6.

[21] I. Kotenko, A. Konovalov, A.Shorov, (2010) “Agent-Based modeling and Simulation of Botnets and Botnet Defence”, Proceeding of Conference on Cyber Conflict (CCD COE).

[22] Myroslav Komar, Anatoliy Sachenko, Sergei Bezobrazov, Vladimir Golovko Intelligent Cyber Defense System ICTERI,2016.

BIOGRAPHIES

"Kushagra Pal is pursuing MBA(Tech.) with specialization in Information Technology from Mukesh Patel School of Technology Management and Engineering ,Narsee Monjee Institute of Management Studies , Mumbai , Maharashtra , India"

"Roopam Tiwari is pursuing MBA(Tech.) with specialization in Information Technology from Mukesh Patel School of Technology Management and Engineering ,Narsee Monjee Institute of Management Studies , Mumbai, Maharashtra , India"

"Shivam Maheshwary is pursuing MBA(Tech.) with specialization in Information Technology from Mukesh Patel School of Technology Management and Engineering ,Narsee Monjee Institute of Management Studies , Mumbai , Maharashtra , India"